

REMARKS/ARGUMENTS

The Office Action has been carefully considered. Claims 1-2, 12, 17, 34-35, 47, and 49-50 are currently amended. Claims 7, 20-33, 37, 40, 44, 53, and 55 are cancelled. Claims 1-6, 8-19, 34-36, 38-39, 41-43, 45-52, 54, and 56-61 are pending. In the Office Action, claims were rejected in the following manner.

1. Claims 1-4, 8-9, 11-19, 31, 34-36, 38-39, 41-42, 45-52, 54, 56-57, and 59-61 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Nonaka et al's US Publication No. 2003/0046238 (hereinafter "*Nonaka*") in view of Hall et al's US Patent No. 7,062,500 (hereinafter "*Hall*") and further in view of Hardy et al's US Patent No. 6,079,018 (hereinafter "*Hardy*") and Thoma et al's US Publication No. 2002/0152393 (hereinafter "*Thoma*").
2. Claims 5-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka*, *Hall*, *Hardy*, *Thoma*, and further in view of Serret-Avila et al's US Patent No. 6,959,384 (hereinafter "*Serret-Avila*").
3. Claims 10, 32-33, 43 and 58 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka*, *Hall*, *Hardy*, *Thoma* and further in view of Chase Jr. et al's US Patent No. 7,080,043 (hereinafter "*Chase*").

35 U.S.C. § 103(a) Rejections

Claims 1-4, 8-9, 11-19, 31, 34-36, 38-39, 41-42, 45-52, 54, 56-57, and 59-61

Claims 1-4, 8-9, 11-19, 31, 34-36, 38-39, 41-42, 45-52, 54, 56-57, and 59-61 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka* in view of *Hall* and further in view of *Hardy* and *Thoma*. Although Applicant does not agree with the rejections, Applicant has nonetheless amended Claims 1-2, 12, 34-35, and 49-50 to clarify the nature of the claimed subject matter.

Amended Claim 1 claims a method comprising:

- obtaining clear form rights information at a client device, said clear form rights information being associated with content stored at said client device;
- obtaining, by said client device, an external key comprising an integrity secret, wherein said integrity secret is vulnerable based at least in part on its being known to at least an external server device;
- obtaining a clear form external integrity hash of first data comprising:
 - said clear form rights information and
 - said external key,

wherein said clear form external integrity hash is vulnerable based at least in part on said vulnerability of said externally-known integrity secret;
obtaining an internal integrity hash of second data comprising
 said clear form rights information,
 said clear form external integrity hash, and
 an externally inaccessible client device key,
 wherein said externally inaccessible client device key is not accessible outside said client device and said internal integrity hash is not vulnerable based on said vulnerability of said externally-known integrity secret;
encrypting said internal integrity hash using said externally inaccessible client device key; and
storing the encrypted internal integrity hash on the client device.

Thus, amended Claim 1 claims a particular combination of secrets, licenses, and hashes that enables a client device to store rights information in clear form, while maintaining an internal integrity hash that is secure despite the vulnerability of externally-known integrity secret. As disclosed in Applicant's specification at page 6 lines 7-13:

In order to use hash 120 to test the integrity of license 110, external secret 122 is known external to the client device. Any of a variety of approaches can be used to try to maintain the security of secret 122, but, unfortunately, any secret known outside the client device is likely to be vulnerable. A sophisticated and determined user is likely to gain access to secret 122 eventually. But, even if hash 120 is compromised, the illustrated embodiment includes a second layer of security and integrity that does not rely on an externally known secret, namely internal security block 130.

In the Office Action at 3, it states, "[i]t appears to the Examiner that the hash within a hash is one of the innovative concepts Applicant is attempting to patent...." Amended Claim 1 clarifies that this appearance was inaccurate. Amended Claim 1 is not directed to a "hash within a hash." Rather, amended Claim 1 is directed in part to obtaining an external integrity hash including rights information and an external key (which includes an integrity secret known outside the device, causing the key, and by extension the external integrity hash, to be vulnerable to discovery by a sophisticated and determined user), and further obtaining an internal integrity hash including the external integrity hash and an externally-inaccessible client device key, thereby "curing" the vulnerability imparted by the externally-known integrity secret.

To sum up, while it is true that a "hash within a hash" is one of several building blocks of the method claimed in Claim 1, the "innovative concept" lies in the particularly claimed combination of various building blocks, including various forms of rights information, various

externally accessible and externally inaccessible secrets or keys, a particular pattern of hashes, and encryption.

Applicant is not attempting to patent a “hash within a hash” in isolation any more than Applicant is attempting to patent encryption in isolation. On the contrary, Claim 1 combines a particularly combined structure that is neither taught nor suggested by the cited art, notwithstanding that some individual pieces of art may disclose one or more of the building blocks from which Claim 1 is constructed. As such Applicant respectfully submits that amended Claim 1 is allowable over the cited art, whether such art is considered individually or in any combination. Amended Claims 34 and 49 recite similar elements and are similarly allowable. Claims 2-4, 8-9, 11-19 31, 35-36, 38-39, 41-42, 45-48, 50-52, 54, 56-57, and 59-61 depend from allowable Claim 1 and are therefore allowable at least by dependency.

Claims 5-6

Claims 5-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma*, and further in view of *Serret-Avila*. Applicant respectfully submits that Claims 5-6 are allowable at least by dependency. Applicant further respectfully submits that *Nonaka, Hall, Hardy, Thoma*, and *Serret-Avila*, alone or in any combination, fail to teach or suggest each element of Claims 5-6 and that Claims 5-6 are therefore allowable according to reasoning similar to that set out above.

Claims 10, 32-33, 43 and 58

Claims 10, 32-33, 43 and 58 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma* and further in view of *Chase*. Applicant respectfully submits that Claims 10, 32-33, 43 and 58 are allowable at least by dependency. Applicant further respectfully submits that that *Nonaka, Hall, Hardy, Thoma*, and *Chase*, alone or in any combination, fail to teach or suggest each element of Claims 10, 32-33, 43 and 58 and that Claims 10, 32-33, 43 and 58 are therefore allowable according to reasoning similar to that set out above.

CONCLUSION

For at least the reasons above, Applicant respectfully submits that all pending claims are allowable and request that the Examiner permit these claims to proceed to issuance. Although additional arguments are believed to exist for distinguishing the cited documents, the arguments presented are believed sufficient to address the Examiner's rejections. Likewise, failure of the Applicant to respond to a position taken by the Examiner is not an indication of acceptance or acquiescence of the Examiner's position. Instead, it is believed that the Examiner's positions are rendered moot by the foregoing arguments, and it is therefore not believed necessary to respond to every position taken by the Examiner with which Applicant does not agree.

The Examiner is respectfully requested to contact the undersigned at the telephone number below if there are any remaining questions regarding this application.

We believe the appropriate fees accompany this transmission. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to AXIOS Law's deposit account. The deposit account number is 50-4051.

Respectfully submitted,
AXIOS LAW

Date: January 25, 2010

by: /Adam L.K. Philipp/

Adam L.K. Philipp - Reg. No.: 42,071
Direct: 206.217.2226
E-mail: adam@axioslaw.com

AXIOS Law
1525 4th Avenue, Suite 800
Seattle, WA 98101
Telephone: 206-217-2200
Customer No.: 61,857